Japanese Publication for Unexamined Patent Application No. 69571/2000 (Tokukai 2000-69571)

A. Relevance of the Above-identified Document

This document has relevance to claims 1 and 16 of the present application.

B. Translation of the Relevant Passages of the Document

[CLAIMS]

[CLAIM 1]

A process for remote and secure payment..., comprising the step of...;

making sure that the buyer is a subscriber correctly registered...

[CLAIM 3]

The process according to claim 2,... comprising the steps of...;

generating a subscriber's electronic signature with an individual authentication algorithm...

[CLAIM 6]

The process according to claim 4, wherein said authentication of the buyer and purchase confirmation comprises the step of:

inputting a secret payment code into the mobile radiotelephone by the buyer...

This Page Blank (uspto)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－69571
（P2000－69571A）
(43)公開日　平成12年３月３日(2000.3.3)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
H04Q 7/38		H04B 7/26	109H	
G06F 17/60		G06F 15/21	340A	
19/00		15/30	C	
H04L 12/28			L	
		H04B 7/26	109S	

審査請求　未請求　請求項の数22　ＯＬ　外国語出願　（全 35 頁）　最終頁に続く

(21)出願番号　特願平11－167748

(22)出願日　平成11年６月15日(1999.6.15)

(31)優先権主張番号　９８０７６６６
(32)優先日　平成10年６月15日(1998.6.15)
(33)優先権主張国　フランス（ＦＲ）
(31)優先権主張番号　９８１３４７１
(32)優先日　平成10年10月23日(1998.10.23)
(33)優先権主張国　フランス（ＦＲ）

(71)出願人　599082609
ソシエテ・フランセーズ・デュ・ラディオテレフォン
フランス国、92915　パリ・ラ・デファンス、プラース・カルボー　1
(72)発明者　アルノー・カピタン
フランス国、45650　サン・ジャン－ル－プラン、アレ・ドゥ・ラ・プレード　1
(72)発明者　クリストフ・フランソワ
フランス国、92200　ヌイイー－シュル－セーヌ、リュ・ジャック・デュリュ　63
(74)代理人　100060069
弁理士　奥山　尚男　（外３名）
最終頁に続く

(54)【発明の名称】　移動無線電話を通して購入した商品及び／又は受けたサービスの遠隔支払いを安全確実に行う方法、システム、及び移動無線電話

(57)【要約】
【課題】　移動無線電話を使用して購入した商品及び／又は受けるサービスの遠隔支払いを安全確実に行う方法とそのシステムと移動無線電話を提供する。
【解決手段】　管理センター（６）及び／又は支払いサーバ（４）及び／又はコントロール・センターによって購入者（２）を識別する（６２）ステップを含む、購入者（２）が供給者（７）から購入した商品及び／又は受けたサービスに対する遠隔支払いを、前記購入者が移動無線電話（１）の使用して安全確実に行う方法を特徴とする。

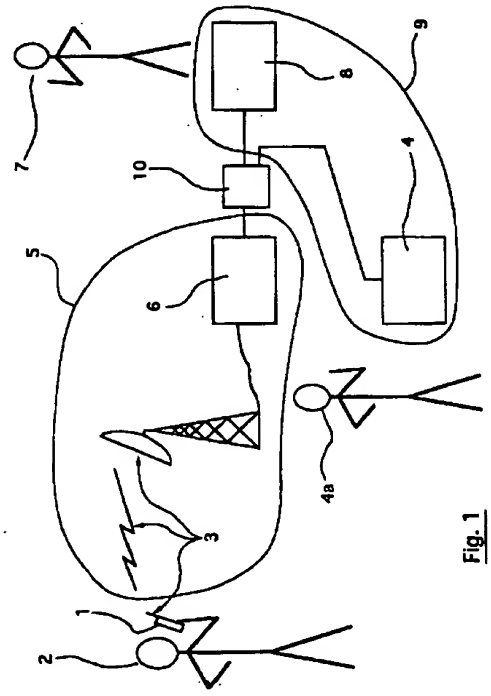

Fig. 1

【特許請求の範囲】

【請求項１】　購入者（２）が供給者（７）から購入した商品及び／又は受けたサービスに対する遠隔支払いを、前記購入者が移動無線電話（１）の使用して安全確実に行う方法であって、ここで、前記移動無線電話が管理センター（６）によって管理されている無線通信ネットワーク（５）にアクセスすることができ、支払いサーバ（４）が無線通信ネットワーク（５）に接続されており、

前記管理センター（６）及び／又は前記支払いサーバ（４）及び／又はコントロール・センターによって前記購入者（２）を識別するステップ（６２）であって、購入者が前記無線通信ネットワーク（５）の加入者リストに正しく登録された者であることを確認する購入者識別ステップを含むことを特徴とする遠隔支払いを安全確実に行う方法。

【請求項２】　前記購入者識別ステップ（６２）が、

前記無線通信ネットワークのユーザとして、前記購入者に個有の加入者識別子（IMSI;23a;50）を、前記管理センター（６）及び／又は前記支払いサーバ（４）及び／又は前記コントロール・センターに受け取らせる加入者識別ステップ（６２ａ）と、

前記加入者識別ステップ（６２ａ）で送られた前記加入者識別子を、前記管理センター（６）及び／又は前記支払いサーバ（４）及び／又は前記コントロール・センターが検査できるようにする加入者認証ステップ（６２ｂ）とを順に含んでなることを特徴とする、請求項１に記載の方法。

【請求項３】　前記加入者認証ステップ（６２ｂ）が、

前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが乱数（５１ａ）を前記移動無線電話へ与えるステップと、

前記移動無線電話が、移動無線電話（１）の保護領域（２３）に含まれる個人認証アルゴリズム（２３ｂ）及び／又は個人認証キー（２３ｃ）を用い、前記乱数を使用して、加入者の電子署名（５１ｂ）を生成するステップと、

移動無線電話が、前記加入者の電子署名を、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターへ送信するステップと、

前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが前記加入者の電子署名を検査するステップとからなることを特徴とする、請求項２に記載の方法。

【請求項４】　前記管理センター（６）及び／又は前記支払いサーバ（４）及び／又は前記コントロール・センターが前記購入者（２）を認証し、場合によっては購入者（２）による商品の購入及び／又はサービスを受ける決定を認証するステップ（６３）を更に含むことを特徴とする請求項１から３のいずれかの１つに記載の方法。

【請求項５】　前記購入者と購入決定の認証ステップが、

移動無線電話が購入者の電子署名を生成するステップと、

移動無線電話が、前記購入者の電子署名を、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターへ送るステップ（２９ａ）と、

前記管理センター及び／又は前記支払いサーバ（４）及び／又は前記コントロール・センターが前記購入者の電子署名を検査し（４２）、この購入者の電子署名が購入者及び供給者により使用できるように維持される（４３、４４）ステップとを含むことを特徴とする、請求項４に記載の方法。

【請求項６】　前記購入者と購入決定の認証ステップが、

購入者が、移動無線電話（１）に関連づけられたキーパッド（２４）を使用して、秘密支払いコードを移動無線電話（１）へ入力するステップと、

移動無線電話が、前記秘密支払いコードを、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターへ安全確実に伝送するステップと、

前記管理センター及び／又は前記支払いサーバ（４）及び／又は前記コントロール・センターが前記秘密支払いコードを検査するステップとを含むことを特徴とする、請求項４に記載の方法。

【請求項７】　前記購入者と購入決定の認証ステップが、

購入者が、移動無線電話（１）に関連づけられたキーパッド（２４）を使用して、秘密支払いコードを移動無線電話（１）に入力するステップを予備ステップとして含むことを特徴とする、請求項５に記載の方法。

【請求項８】　前記秘密支払いコードを入力する前記ステップが、前記移動無線電話に記憶された入力アルゴリズムを使用してなされることを特徴とする、請求項６又は７のいずれかに記載の方法。

【請求項９】　前記秘密支払いコードが入力される前記ステップが、この目的のために提供されるＨＤＭＬ又は同等フォーマットの少なくとも１つのダウンロード・ページを使用してなされることを特徴とする、請求項６又は７のいずれかに記載の方法。

【請求項１０】　購入者の電子署名が生成される前記ステップが、

移動無線電話（１）の保護領域（２３）に含まれる支払いセキュリティ・アルゴリズム（２３ｄ）及び／又は支払いセキュリティ・キー（２３ｅ）を使用するステップと、

取引に関するデータ及び／又は購入者に関するデータから出発するステップとによって実行されることを特徴とする請求項５、又は７から９のいずれか１つに記載の方法。

【請求項１１】　取引に関する前記データの少なくともいくつかのデータが変動性を含むことを特徴とする、請求項１０に記載の方法。

【請求項１２】　前記移動無線電話（１）が加入者識別モジュール（２３）と協働する端末（２０）を含んでおり、前記支払いセキュリティ・アルゴリズム及び／又は前記支払い・セキュリティ・キーが前記端末の保護領域に記憶されていることを特徴とする、請求項１０又は１１の何れかに記載の方法。

【請求項１３】　前記移動無線電話（１）が加入者識別モジュール（２３）と協働する端末（２０）を含んでおり、前記支払いセキュリティ・アルゴリズム（２３ｄ）及び／又は前記支払い・セキュリティ・キー（２３ｅ）が前記加入者識別モジュールの保護領域に記憶されていることを特徴とする、請求項１０又は１１のいずれかに記載の方法。

【請求項１４】　移動無線電話（１）の保護領域（２３）に含まれる秘密識別コード（ＰＩＮコード）と、購入者によってキーパッド（２４）を使用して移動無線電話へ入力される購入者が知っている秘密キーとの比較が一致したとき、移動無線電話（１）がロック解除されるステップ（６１）を更に含むことを特徴とする、請求項１から１３のいずれか１つに記載の方法。

【請求項１５】　前記移動無線電話（１）が加入者識別モジュール（２３）と協働する端末（２０）を含んでおり、移動無線電話（１）の前記保護領域の少なくともいくつかが前記加入者識別モジュールに含まれることを特徴とする、請求項３、又は１０から１２のいずれか１つに記載の方法。

【請求項１６】　買い物が秘密であることを安全確実に行うため、購入した及び／又は受けたサービスの支払いの関連データが暗号化され（２９１）、移動無線電話と管理センター及び／又は支払いサーバ及び／又はコントロール・センターの間で交換されるステップを更に含むことを特徴とする請求項１から１５のいずれか１つに記載の方法。

【請求項１７】　詐欺者がデータを変更することができないように、移動無線電話と管理センター及び／又は支払いサーバ及び／又はコントロール・センターの間で交換される、購入した商品及び／又は受けたサービスの支払いの関連データの完全性を検査するステップ（２９２）を更に含むことを特徴とする、請求項１から１６のいずれかの１つに記載の方法。

【請求項１８】前記購入者が、
前記無線通信ネットワークのユーザとしての前記購入者に個有の加入者識別子（ＩＭＳＩ；２３ａ；５０）に関連づけられた電子財布識別子（７１）と、
支払い手段（７３、７３ａ、７３ｂ、７３ｃ）と、
前記購入者に関する情報（７４）及び／又は前記購入者の口座とを含んでなる電子財布（７０）に関連づけられ、
特に、商品を購入及び／又はサービスを受けるときに、購入者が成功裏に識別され（６２）、場合によっては認証される（６３）まで、前記支払い手段（７３）の使用が許可されないことを特徴とする、請求項１から１７のいずれか１つに記載の方法。

【請求項１９】　前記電子財布（７０）が、前記購入者が知っている秘密支払いコード（７２）を更に含むことを特徴とする、請求項１８に記載の方法。

【請求項２０】　前記移動無線電話（１）が加入者識別モジュール（２３）と協働する端末（２０）を含んでおり、
前記電子財布（７０）が、
前記端末（２０）と、
前記加入者識別モジュール（２３）と、
前記支払いサーバ（４）と、
前記管理センター（６）と、
前記コントロール・センターとから成るグループに属する要素の１つに記憶されていることを特徴とする、請求項１８又は１９のいずれかに記載の方法。

【請求項２１】　購入者（２）が供給者（７）から購入した商品及び／又は受けたサービスの遠隔支払いを、前記購入者（２）に使用される移動無線電話（１）を使用して安全確実に行い、前記移動無線電話が管理センター（６）によって管理される無線通信ネットワーク（５）へのアクセスを提供し、支払いサーバ（４）が前記無線通信ネットワークに接続されているシステムであって、請求項１から２０のいずれか１つに記載の方法を実現する手段を含むことを特徴とする遠隔支払いを安全確実に行うシステム。

【請求項２２】　購入者（２）が供給者（７）から購入した商品及び／又は受けたサービスの遠隔支払いを、前記購入者（２）に使用される移動無線電話（１）を使用して安全確実に行うために購入者に使用される移動無線電話（１）であって、この移動無線電話が管理センター（６）によって管理される無線通信ネットワーク（５）へのアクセスを提供し、支払いサーバ（４）が前記無線通信ネットワークに接続されており、前記移動無線電話は請求項１から２０のいずれか１つに記載の方法を実現する手段を含むことを特徴とする、遠隔支払いを安全確実に行うための移動無線電話。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、移動無線電話を使用して購入した商品及び／又は受けたサービスの遠隔支払いを行う方法に関する。更に、本発明は、この方法を実現するためのシステム及び移動無線電話に関する。本発明はすべてのタイプの移動無線電話に、言い換えれば、端末のみを有する無線電話と加入者識別モジュールと連動する端末を有する移動無線電話に適用される。

【０００２】
【従来の技術】ＧＳＭ標準では、移動無線電話（「移動ステーション」とも呼ばれる）は第２のタイプに属し、そこで使用される端末及び加入者識別モジュールはそれぞれ「移動機器」及び「ＳＩＭ（Subscribe Identification Module:加入者識別モジュール）」と呼ばれる。ＳＩＭカードは、移動無線電話の中へ差し込まれるマイクロプロセッサ・カードの形式であることに注目されたい。それは加入者特有のすべての個人情報、特に加入者の国際モジュール加入者識別子（International Modules Subscriber Identity:ＩＭＳＩ）、個人認証キー（Ｋｉと呼ばれる）、及び個人認証アルゴリズム（Ａ３／Ａ８と呼ばれる）を含んでいる。
【０００３】各種の電子支払い方法及びシステムが、既に提案されている。１９９１年１０月９日に発行された欧州特許公報第ＥＰ４５１０５７Ｂ１号は、支払いサーバの使用で構築する方法とシステムを説明している。この特許で提案されるソリューションは、音声識別信号を送るカードの使用を含んでいる。この信号は電話マイクロホンによって受け取られ、次に支払いサーバへ送られる。更に、１９９６年１０月１７日に発行された国際特許公報第ＷＯ９６／３２７０１号は、支払いサーバの使用で構築する電子支払い方法を説明している。それは、販売サーバ・ステーション及び顧客ステーション及び支払いサーバ・ステーションが接続された、例えば「インターネット」ネットワークのようなオープン・コンピュータ・テレコミュニケーション・ネットワークを介するＩＴサービスによって、販売者によって提供される商品の購入に関連した取引（トランザクション）を行うために使用することができる。
【０００４】本発明の目的は、移動無線電話を介する買い物又は受けたサービスの遠隔支払いは、クローズド・タイプ（closed type）の無線通信ネットワークを介してなされるものと想定されている。クローズド・タイプの無線通信ネットワークとは、他を排除する意味ではなく、例えば、ＧＳＭテクノロジー（例えば、ＧＳＭ９００、ＤＣＳ１８００、など）に基づくネットワークを意味している。
【０００５】クローズドな無線通信ネットワークは、明らかにプラットフォーム又はゲートウエイを介して１つ（又は複数の）オープン・ネットワークに接続されることができる。従って、クローズドな無線通信ネットワークのユーザは、オープン・ネットワークにアクセスするため、それ自体の移動無線電話を使用することができる。例えば、「インターネット」のようなオープン・ネットワークは、もし移動無線電話がＨＤＭＬ（Handset Device Markup Language）又はＷＭＬ（WirelessMarkup Language）又は同じタイプ及び／又は上記２つの言語の１つから由来した他の言語のような特殊言語に基づいたプロトコルを使用する手段（例えば、ナビゲータ又はブラウザ）を有していれば、ＧＳＭネットワークから移動無線電話を使用してアクセスすることができる。
【０００６】クローズドな無線通信ネットワークはオープン・コンピュータ・テレコミュニケーション・ネットワークのカテゴリーに入らないので、国際特許公報第ＷＯ９６／３２７０１号において推奨される解決法は、本発明に関連する問題（特に、移動無線電話を使用して買い物又は受けるサービスの遠隔支払い）に適用することができない。
【０００７】
【発明が解決しようとする課題】本発明の目的は、移動無線電話を使用して構築する、供給者から購入した商品及び／又は受けたサービスの遠隔支払いを安全確実に行う方法を提供することである。本発明の他の目的は、最適の安全性を提供しながら、購入者によってなされる作業を最小限にする支払い方法を提供することである。
【０００８】
【課題を解決するための手段】これらの様々な目的及び後に明らかになる他の目的は、本発明に従って、購入者によって使用される移動無線電話を使用して、供給者から購入者が購入した商品及び／又は受けたサービスの遠隔支払いを安全確実に行う方法によって達成されるが、その場合、前記移動無線電話は管理センターによって管理される無線通信ネットワークにアクセスすることができ、支払いサーバが前記無線通信ネットワークに接続されており、前記方法は前記管理センター及び／又は前記支払いサーバ及び／又はコントロール・センターによって、購入者が前記無線通信ネットワークへの加入者リストに正しく登録された加入者であることを確認することから構成される前記購入者を識別するステップを含んでなる。
【０００９】そして、この購入者識別ステップの終わりに、購入者は支払いサーバが接続された無線通信ネットワークの真正なメンバーであることを、支払いサーバにより保証される。注意すべきなのは、もし購入者が無線通信ネットワークの管理センターによって識別されるならば、無線通信の提供者（この管理センターの運用に責任を有する者）は、銀行（支払いサーバの運用に責任を有する者）に対して、本発明のフレームワークの中では、「半ば信頼された第三者（semi-trusted third party）」となることである。この場合、銀行は購入者を単純に認証し、無線通信の提供者は移動無線電話を所持する人物の識別に責任を有する。
【００１０】前記の購入者識別ステップは、それ自体が、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが、前記無線通信ネットワークの使用者としての前記購入者に個有の加入者識別子を受け取ることができるようにする加入者識別ステップと、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターに、前記加入

者識別ステップの間に送られた前記加入者識別子を検査させる加入者認証ステップとを順次に含んでなることが好ましい。

【００１１】このように、本発明は、最初の購入者識別ステップの間に、クローズドな無線通信ネットワーク（例えば、ＧＳＭタイプ）の加入者は、詐欺を防止し請求が正しいものであることを保証するため、請求システムに責任のある無線通信の提供者によって識別され認証されなければならないという利点がある。従って、クローズド・ネットワーク、例えばＧＳＭタイプの物理層によって提供されるセキュリティが巧に使用されている。（これに対し、）インターネットのようなオープン・ネットワークでは、セキュリティはアプリケーション・レベルで与えられることに注意されたい。

【００１２】前記加入者認証ステップは、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが前記移動無線電話に乱数（ランダムな数）を与えるステップと、移動無線電話の保護された領域に含まれる個人認証アルゴリズム及び／又は個人認証キーを用いて、前記乱数を使用して、前記移動無線電話が加入者の電子署名を生成するステップと、移動無線電話が、前記加入者の電子署名を前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターへ送信するステップと、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが前記加入者の電子署名を検査するステップとを含んでなることが好ましい。

【００１３】このようにして、ＧＳＭ標準により規定された加入者認証手順が、購入者識別ステップの間に使用される。特に重要な点は、加入者認証手順がいかなる場合でも購入者認証手順と混同されてはならないことである。前記の方法は、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが、前記購入者と購入者による商品の購入及び／又はサービスを受ける決定を認証するステップを含むことがさらに好ましい。

【００１４】このように、この購入者認証ステップの終わりに、支払いサーバ・マネージャは、購入者が購入する商品及び／又は受けるサービスを支払うことが許可されていることを保証する。従って、支払いサーバ・マネージャは支払いを許可するか、購入者の口座と供給者の口座との間で対価の移動（compensation movements）を行うことができる。

【００１５】本発明では、前記購入者と購入決定認証ステップは、それ自体が、移動無線電話が、購入者の電子署名を生成するステップと、移動無線電話が、前記購入者の電子署名を、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターへ送信するステップと、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが、前記購入者の電子署名を検査して、前記購入者の電子署名が購入者及び供給者により使用できるように維持されるステップとを含んでなるのが好ましい実施形態の１つである。

【００１６】前記購入者と購入決定認証ステップは、それ自体が、購入者が、移動無線電話に付属のキーパッドを使用して、秘密支払いコードを移動無線電話へ入力するステップと、移動無線電話が、前記秘密支払いコードを、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターへ安全確実に伝送するステップと、前記管理センター及び／又は前記支払いサーバ及び／又は前記コントロール・センターが、前記秘密支払いコードを検査するステップとを含んでなるのが本発明の１つの好ましい実施形態である。

【００１７】従って、この実施態様に従えば、署名を計算する必要はない。例えば、安全確実な伝送は暗号化形式での伝送であることができる。前記購入者と購入決定認証ステップは、購入者が、秘密支払いコードを、移動無線電話に付属のキーパッドによって移動無線電話へ入力するステップを含むことが有利である。具体的には、前記購入者の電子署名は前記秘密支払いコードの関数として生成されることができる。この任意なステップは、購入者が認証されるセキュリティを増進させる。

【００１８】秘密支払いコードを入力するこのステップは、２つ好ましい実施形態が考えられる。第１の実施態様では、このステップは前記移動無線電話に記憶された入力アルゴリズムを使用して実行される。従って、この第１の変形例では、移動無線電話は入力アルゴリズムを永久的に記憶する（端末及び／又は加入者識別モジュールの中に）。従って、それは無線電話装置における（端末及び／又は加入者識別モジュールの中で）若干の変更を必要とする。

【００１９】第２の実施態様では、このステップはＨＤＭＬ又はこの目的のために提供される同等のフォーマットによる少なくとも１つのダウンロードされたページを使用して実行される。従って、この第２の実施態様では、無線電話は入力アルゴリズム用の永久的な記憶領域を含まない。購入者の電子署名が生成される前記ステップは、移動無線電話の保護領域に含まれる支払いセキュリティ・アルゴリズム及び／又は支払い・セキュリティ・キーを用いて、取引に関連したデータ及び／又は購入者に関するデータから出発することによってなされることが好ましい。

【００２０】購入者の電子署名は、取引に関連するデータを考慮するかどうかに依存して、購入者のみを認証するか、購入者及び購入決定の双方を認証することに注意されたい。これは購入者及び／又は供給者及び／又は支払いサーバの間の紛争を調停するために使用することができるので、紛争が生じた場合に不可欠である。取引に関連した前記データの少なくとも或るものは可変情報を

含むことが好ましい。前記支払いセキュリティ・アルゴリズム及び／又は前記支払い・セキュリティ・キーは、前記端末の保護された領域に記憶されることが好ましい。１つ好ましい実施形態に従えば、データは前記加入者識別モジュールの保護された領域に記憶されることになる。

【００２１】前記方法は更に次のステップを含むことが好ましい。即ち、もし移動無線電話の保護領域に含まれる秘密識別コードと、購入者に知られ且つ購入者によってキーパッドを使用して移動無線電話へ入力された秘密キーとの比較が一致すれば、移動無線電話をアンロックまたはロック解除するステップである。移動無線電話のこの「アンロック」又は「ロック解除」（「初期化」とも呼ばれる）は、それ自体既知の付加的なオプションである確認であり、特にＧＳＭタイプのネットワークでは或る無線通信の提供者によって提供される。注意すべきなのは、例えば、加入者識別モジュールが端末に挿入される度に、又は端末がスイッチを入れられる度に、個人識別番号（又はＰＩＮコード）が加入者によって入力されることである。

【００２２】移動無線電話の前記保護領域の少なくとも或るものが、加入者識別モジュールの中に含まれることが好ましい。セキュリティの確保を理由として、端末をできるだけユーザから独立させるために、最大量の個人及び秘密情報（アルゴリズム及び個人認証キー、支払いアルゴリズム、及びセキュリティ・キーなど）を加入者識別モジュールの中に限定的に格納するのが好ましい。前記方法は、更に購入が秘密に保たれることを保証するために、商品の購入及び／又はサービスの受領の支払い関連データを暗号化し、移動無線電話と、管理センター及び／又は支払いサーバ及び／又はコントロール・センターとの間で交換するステップを含むことが好ましい。

【００２３】前記方法は、更に詐欺者がデータを変更することができないように、移動無線電話と、管理センター及び／又は支払いサーバ及び／又はコントロール・センターとの間で交換される商品及び／又はサービス購入の支払い関連データの完全性を検査するステップを含むことが好ましい。本発明の好ましい実施形態において、前記購入者は、前記無線通信ネットワークのユーザとしての前記購入者に特定した加入者識別子に関連づけられた財布識別子と、支払い手段と、前記購入者及び／又は前記購入者の口座に関する情報と、を含んでなる電子財布（electronic wallet）に関連づけられ、前記支払い手段は、特に商品の購入及び／又はサービスの受領があったとき、購入者が成功裏に識別されまで、あるいは場合によっては承認されるまで使用が許可されない。

【００２４】（もし必要ならば）購入者の識別及び認証は、この購入者の電子財布の識別及び認証（もし適用可能であれば）としても見ることができる。例えば、１人の加入者（及び対応する加入者識別モジュール）が単一の電子財布に関連づけられる場合や、数人の加入者（従って、幾つかの対応する加入者識別モジュール）が同一の電子財布を共用する場合（例えば、会社が財布を保有する場合）、１人の加入者（及び対応する加入者識別モジュール）が幾つかの電子財布に関連づけられる場合などのいくつかの場合が生じる。

【００２５】財布識別子（wallet identifier）と加入者識別子（subscriber identifier）の間の相関関係のために（加入者が購入者である）、購入者（加入者として）の識別は、その購入者の電子財布の暗黙の識別を与えることに注意されたい。前記の第３の場合、加入者の電子財布の１つが、例えばデフォルトによって選択されるか、変形として、購入者は利用可能な幾つかの電子財布から選択する能力を与えられてよいことに注意されたい。識別後、そして場合によっては認証後に、購入者はその電子財布に含まれる支払い手段を使用することができる。

【００２６】前記電子財布も前記購入者に知られた秘密支払いコードを含むことが好ましい。注意すべきなのは、購入者によって無線電話キーパッドを使用して入力されたこの秘密支払いコードは、購入者及び購入決定が認証されるように、購入者の電子署名の計算に使用されてよいことである。前記電子財布は、前記端末、前記加入者識別モジュール、前記支払いサーバ、前記管理センター、及び前記コントロール・センターから構成されるグループに属する要素の１つに記憶されることが好ましい。

【００２７】言い換えれば、本発明のフレームワークの外側に逸脱しない限り、電子財布（electronic wallet）の様々な配置を考えることができる。更に、本発明は、購入者によって使用される移動無線電話を使用して、購入者が供給者から購入する商品及び／又は受けるサービスの安全確実な遠隔支払いを行うシステムに関連している。更に、本発明は、供給者から購入者によって購入する商品及び／又は受けるサービスについて確実に遠隔支払いを行うため購入者によって使用される移動無線電話に関連している。

【００２８】本発明に従ったシステム及びこの無線電話は、前述した方法を具体化する手段を含んである。本発明の他の特徴及び利点は、以下の異なった各種の実施形態の説明及び添付の図面から明らかとなるであろう。本発明はこれらの実施態様及び目的に限られない。

【００２９】

【発明の実施の形態】本発明は、購入者が移動無線電話を使用して商品を購入及び／又はサービスを受けるときに遠隔支払いを行うために使用することのできる方法、対応するシステム及び移動無線電話に関する。図１に示される好ましい実施形態において、システムは、無線中継リンク３を介して、管理センター６によって管理される無線通信ネットワーク５（例えば、ＧＳＭネットワー

ク）にアクセスすることのできる移動無線電話１を含む。更に、支払いサーバ４及び販売サーバ８が無線通信ネットワーク５に接続されている。

【００３０】図示された例において、支払いサーバ４及び販売サーバ８はオープン・コンピュータ・テレコミュニケーション・ネットワーク、例えば、インターネット・ネットワーク９へ接続されている。無線通信ネットワーク５は、ゲートウエイ１０（例えば、アンワイヤード・プラネット社（Unwired Planet Company）から市販されているＵＰアクセス・プラットフォーム）を介してこのインターネット・ネットワーク９へ相互接続される。この場合、移動無線電話には、ゲートウエイを介して、インターネット・ネットワーク内で移動無線電話をナビゲートし、特に支払いサーバ４及び販売サーバ８にアクセスすることのできるナビゲータ（例えば、アンワイヤード・プラネット社から市販されている「UP browser」（登録商標）のナビゲータ）が設けられる。

【００３１】従って、このシステムの場合は、無線通信ネットワーク５に登録された加入者と想定される移動無線電話１を有する購入者２に、遠隔の販売サーバ８を有する供給者７から購入した商品及び／又は受けたサービスについて安全確実な遠隔支払いを可能にできる。図２に示された好ましい実施形態において、移動無線電話１はＳＩＭカード２３と協働して働く端末２０を含む。しかし、本発明は端末のみから構成される（言い換えれば、加入者識別モジュールを含んでいない）無線電話に対しても適用可能であることは明らかである。

【００３２】周知のように、端末２０は、例えば、通信管理モジュール２１及び情報処理手段２９を含み、それらの周りにキーパッド２４、表示スクリーン２６、拡声器２７、マイクロホン２８、及び無線送受信手段２９ａ（アンテナを含む）が相互接続される。ここで提供される情報は、更に、任意タイプの移動無線電話へ一般的に適用可能であることが明らかである。従って、前記の「通常型の」端末は、無線通信ネットワークへ接続することのできる任意タイプの無線通信モジュール、例えば、キーパッド又はスクリーンを有しない端末、又はＰＣＭＣＩＡ（Personal Computer Memory Card International Association）又は同等のタイプのカードを介して端末と協働するマイクロコンピュータと置換されることができる。

【００３３】本発明に従った方法は、図６のフローチャートで示されるように、移動無線電話１を（任意に）アンロックまたはロック解除する（６１）（又は初期設定する）ステップと、管理センター６及び／又は支払いサーバ４及び／又は独立のコントロール・センター（図示されていない）が、購入者を無線通信ネットワークのユーザとして識別する（６２）ステップと、任意のステップとして管理センター６及び／又は支払いサーバ４及び／又はコントロール・センター（図示されていない）が、購入者と商品を購入する及び／又はサービスを受けるために購入者がした購入決定を認証する（６３）とを含んでなる。

【００３４】移動無線電話１がアンロックまたはロック解除される（任意の）ステップ６１は周知であり、例えば、次のように行われる。即ち、購入者２は個人識別番号（又はＧＳＭテクノロジに従ったＰＩＮコード）をキーパッド２４から入力し、次に移動無線電話１が、購入者によって入力された個人識別番号を、移動無線電話１の保護領域（通常はＳＩＭカード２３）に記憶された個人識別番号と比較する。移動無線電話１は、この比較が一致しなければ「アンロック」あるいは「ロック解除」（言い換えれば、無線通信ネットワークの中で動作可能にすること）がなされない。

【００３５】本発明に従って購入者２が識別されるステップ６２は、加入者を識別し認証することから構成され、この加入者は無線電話を使用するときの購入者である。従って、例えば、このステップ６２は、以下の従来からある、加入者の識別ステップ（６２ａ）と、これよって、管理センター６は、無線通信ネットワークのユーザとしての購入者に個有の加入者識別子を受け取り、加入者識別子２３ａ、又はＧＳＭテクノロジーに従ったＩＭＳＩは、通常、ＳＩＭカード２３に記憶され、管理センターが加入者識別ステップ６２ａで送られた加入者識別子を検査できるようにする加入者の認証ステップ（６２ｂ）とを含んでなる。

【００３６】注意すべきことは、購入者識別ステップ（加入者の識別と認証を含む）は、自動的に行われることである。言い換えれば、それは購入者の操作を必要としない。購入者は、その秘密支払いコードの入力を求められたときに、次の購入者認証ステップに関与するのみである。更に重要なことは、加入者認証ステップ６２ｂは、いかなる場合でも、以下で詳細に説明する購入者認証ステップ６３と混同されてはならないことである。加入者（購入者である）の認証は、購入者を識別するためにのみ行われる。この購入者の識別は、識別された購入者が購入を許可されていることを支払いサーバが確認するために、購入者の認証と共に使用されるべきと考えられる。

【００３７】単なる例として、これらの加入者識別ステップ６２ａ及び加入者認証ステップ６２ｂのためにＧＳＭで使用される「通常の」手順を示す図５を参照する。移動無線電話１はユーザの加入者識別子（ＩＭＳＩ）５０を管理センター６へ送る。加入者がこのようにして識別された後に（６２ａ）、管理センター６はその識別を検査しなければならない。言い換えれば、その加入者を認証しなければならない（６２ｂ）。これは、管理センター６が乱数あるいはランダムな数値（「ＲＡＮＤ」）５１ａを移動無線電話１へ与えることによって行われる。この乱数から出発し、移動無線電話の保護領域（通

常は、ＳＩＭカード２３）に含まれるアルゴリズム（「Ａ３／Ａ８」）２３ｂ及び個別認証キー（「Ｋｉ」）２３ｃを使用して、移動無線電話１は加入者の電子署名（「ＳＲＥＳ」）を計算する。

【００３８】この加入者の電子署名５１ｂは管理センター６（もっと正確には、加入者管理モジュール３０）へ送られ、管理センター６は、それを管理センター６において計算した署名と比較することによって、それを検査する。もし２つの加入者電子署名が等しければ、加入者の認証（及び、本発明の目的のためには、購入者の識別）は成功し（移動無線電話１を有する人物は加入者のリストにあること）、管理センターは、これを移動無線電話１及び支払いサーバの中に置かれた識別モジュール４０へ立証するために、メッセージ５１ｃ及び５２を送る。更に、ＧＳＭテクノロジは、ネットワーク・トポロジの機能としてコミュニケーション・セットアップの独立した認証を行わせる（セットアップのとき、ハンドオーバーの間など）。

【００３９】要するに、購入者識別ステップ６２を実行した後で、支払いサーバ４の支払いサーバ・マネージャ４ａは、移動無線電話１を保持している人物（言い換えれば、この場合、購入者２）は、加入者リストに正しく登録されており、かつ、支払いサーバ４が接続されている無線通信ネットワークの真正なメンバーであることを保証される。購入者識別ステップ６２の次に、購入者認証ステップ６３が続く。このステップでは、支払いサーバ４の支払いサーバ・マネージャ４ａは、支払いのときに移動無線電話１を所持している購入者２が、購入した商品及び／又は受けたサービスを支払うことを許可していることを保証する。保証されれば、支払いサーバ・マネージャは、支払いを許可するか、購入者２の口座と供給者７の口座との間の対価の移動を行うことができる。この購入者認証ステップ６３は、購入者が購入決定を行う前、又は行った後に実行することができる。

【００４０】１つの好ましい実施形態において、購入者認証ステップ６３は、

（任意に）購入者２は、秘密支払いコードを入力するために、移動無線電話１の上のキーパッド２４を使用するステップと、例えば、この入力ステップは、移動無線電話（又はＳＩＭカード２３、又は端末２０）に記憶された入力アルゴリズムを使用して実行されるか、その変形の１つによれば、この目的のために提供されるＨＤＭＬ又はそれに同等のフォーマットの１つまたは複数のダウンロードされたページを使用して実行することができ、移動無線電話は購入者の電子署名を生成するステップと、ここで、移動無線電話の保護領域（端末２０又はＳＩＭカード２３）に含まれるアルゴリズム２３ｄ及び支払いセキュリティ・キー２３ｅを使用し、取引に関するデータ（内容及び／又は価格のような）及び／又は購入者に関するデータ（もし購入者が支払いコードを入力したのであれば、秘密支払いコードのような）から始め、更に、取引に関するデータは、署名に変動性を与える要素（例えば、取引の日時、乱数、取引一連番号、など）を含むことができ、移動無線電話１は購入者の電子署名を支払いサーバ４へ送信するステップと、購入者の電子署名が、支払いサーバ４に含まれる検査モジュール４２で検査されるステップと、ここで、購入者の電子署名は、購入者２及び供給者７が使用できるように維持され、更に、この検査は加入者管理センター６又はコントロール・センター（図示されていない）によって実行されてよく、前者の場合、加入者管理センター６は遠隔支払いサービスに加入している無線電話所持者の認証モジュール３３を含むものであり、を含んでなる。

【００４１】次に、好ましい実施形態（例として与えられる）で採用された購入者認証ステップの手順が続く（図５の下部を参照）。購入者２は購入要求５３を供給者７の販売サーバ８へ送る。その見返りに、購入者は商品及び／又はサービス５４の価格に関するデータを受け取る。次に、購入者は購入決定５５を行う。同時に、移動無線電話内の計算手段（通常はマイクロプロセッサ）は、購入者の電子署名を計算する。移動無線電話１は無線送受信手段２９ａを使用して、第１に供給者７の販売サーバ８へ（矢印５５）、第２に支払いサーバ４へ（矢印５６）、購入者の購入決定及び電子署名を送る。支払いサーバ４は購入者の電子署名を検査（又は証明）する検査モジュール（又は証明モジュール）４２を含む。この検査モジュール４２は、例えば、購入のときに移動無線電話で実行された計算動作と全く同じ計算動作を実行することによって署名を検査する。もし支払いサーバ４が取引を受け入れると、支払いサーバ４上の受容通知モジュール４３を介して、「取引許容」メッセージ５７が供給者の販売サーバ８へ送られる。供給者の販売サーバ８は、「購入確認」メッセージ５８を購入者（購入者の移動無線電話及び／又は購入者の家庭）に送る。購入者の電子署名は支払いサーバ４の記憶モジュール４４によって記憶され、購入者及び供給者が利用できるように保持される。

【００４２】もし加入者管理センター６又はコントロール・センター（図示されていない）が購入者の電子署名を検査（又は証明）すると、加入者管理センター又はコントロール・センターは、支払いサーバ４に関して説明したような検査モジュール４２、受容通知モジュール４３、及び記憶モジュール４４のような検査、通知、及び記憶タイプのモジュールを含むことは明らかである。

【００４３】より容易に実施することができる他の変形に従えば、購入者認証ステップ６３、及び場合によっては購入決定自体は、購入者が、移動無線電話に付属のキーパッド２４を使用して、秘密支払いコードを移動無線電話１へ入力するステップと、この入力ステップは、例えば、移動無線電話（ＳＩＭカード２３又は端末２０）

に記憶された入力アルゴリズムを使用して実行するか、１つの変形によれば、この目的に提供されるＨＤＭＬフォーマット又はそれと同等のフォーマットの１つまたは複数のダウンロードされたページを使用して実行することができ、移動無線電話が秘密支払いコードを支払いサーバ４へ安全確実に送信するステップと、支払いサーバ４が秘密支払いコードを検査するステップと（例えば、この秘密支払いコードが実際に有効な支払いコードの所定のリストに属していることを確認することによる）、を含んでなる。

【００４４】どのような実施形態が選択されるかに関わらず、購入者認証ステップ６３の後では、支払いサーバ４の支払いサーバ・マネージャ４ａは、支払い時点で移動無線電話１を所持している購入者２が、購入した商品及び／又は受けたサービスに対して支払うことを許可していることを保証される。購入者の電子署名は、購入者２及び／又は供給者７及び／又は支払いサーバ４の支払いサーバ・マネージャ４ａとの間で生じる紛争を調停するのに十分である。

【００４５】本発明に従えば、移動無線電話１は、例えば通信管理モジュール２１の中に、これまでに（幾つかの実施形態及びその変形で）説明した方法の様々なステップを実現するのに必要な様々な手段を含んでいる。具体的には、無線電話は無線電話をアンロックまたはロック解除するのに必要な手段２２、購入者を識別するのに必要な手段３４、及び購入者を認証するのに必要な手段２５を含んでいる。

【００４６】移動無線電話１の通信管理手段及び／又は情報処理手段２９は、移動無線電話１及び／又は管理センター６及び／又は支払いサーバ４及び／又はコントロール・センターの間で周知の方式で交換される、購入した商品及び／又は受けたサービスの支払いデータを暗号化する手段２９１を含むことができる。これらの暗号化手段は購入の秘密性を保証する。

【００４７】更に、移動無線電話１の情報処理手段２９は、移動無線電話１及び／又は管理センター６及び／又は支払いサーバ４及び／又はコントロール・センターの間で周知の方式で交換される、購入した商品及び／又は受けたサービスの支払い関連データの完全性をコントロールする手段２９２を含むことができる。従って、詐欺者はこのようなデータを変更することはできない。

【００４８】更に、本発明に従えば、各購入者は、電子財布（electronic wallet）７０に関連づけられることができる。図７に示されるように、この電子財布７０は、例えば、購入者（無線通信ネットワークのユーザとしての）に個有の加入者識別子（例えば、加入者の「ＩＭＳＩ」）に関連づけられた財布識別子７１と、購入者２に対してのみ知られている秘密支払いコード７２と、支払い手段７３と、ここで、支払い手段７３は、排他的にではないが、例えば、電子財布７３ａ（通常、所定のしきい値よりも小さな金額について）、クレジット・カード・ホルダー７３ｂ（通常、前記の所定しきい値より大きな金額について）、又は銀行によって提供され購入者が利用できる他の支払い手段７３ｃであり、購入者及び／又はその口座に関する情報７４とを含んでなる。

【００４９】支払い手段７３の使用は、特に購入者２の識別、及び購入する決定の認証が成功した後に、商品及び／又はサービスを購入するときにのみ許可される。この電子財布を様々な場所、即ち、端末２０、ＳＩＭカード２３、支払いサーバ４、管理センター６、又はコントロール・センター（図示されていない）に記憶させることができる。

【図面の簡単な説明】

【図１】本発明に従ったシステムの好ましい実施形態の全体概略図である。

【図２】本発明に従った移動無線電話の好ましい実施形態を示すブロック図である。

【図３】本発明に従った管理センターの好ましい実施形態を示すブロック図である。

【図４】本発明に従った支払いサーバの好ましい実施形態を示すブロック図である。

【図５】商品の購入及び／又は受けるサービスに関連した操作ステップを示す構成図である。

【図６】本発明に従った方法の好ましい実施形態を示す簡略フローチャートである。

【図７】本発明に従った電子財布の好ましい実施形態を示すブロック図である。

【符号の説明】

１	移動無線電話
２	購入者
３	無線中継リンク
４	支払いサーバ
４ａ	支払いサーバ・マネージャ
５	無線通信ネットワーク
６	加入者管理センター
７	供給者
８	販売サーバ
９	インターネット・ネットワーク
１０	ゲートウエイ
２０	端末
２１	通信管理モジュール
２２	手段
２３	ＳＩＭカード
２３ａ	加入者識別子
２３ｂ	アルゴリズム
２３ｃ	認証キー
２３ｄ	アルゴリズム
２３ｅ	支払いセキュリティ・キー
２４	キーパッド
２５	手段

２６	表示スクリーン
２７	拡声器
２８	マイクロホン
２９	情報処理手段
２９ａ	無線送受信手段
３０	加入者管理モジュール
３３	認証モジュール
３４	手段
４０	識別モジュール
４２	検査モジュール
４３	受容通知モジュール
４４	記憶モジュール
５０	加入者識別子
５１ａ	乱数
５１ｂ	電子署名
５１ｃ	メッセージ
５２	メッセージ
５３	購入要求
５４	商品及び／又はサービス
５５	購入決定
５７	「取引許容」メッセージ
５８	「購入確認」メッセージ
７０	電子財布
７１	財布識別子
７２	秘密支払いコード
７３	支払い手段
７３ａ	電子財布
７３ｂ	クレジット・カード・ホルダー
７３ｃ	他の支払い手段
７４	情報
２９１	手段
２９２	手段

【図１】

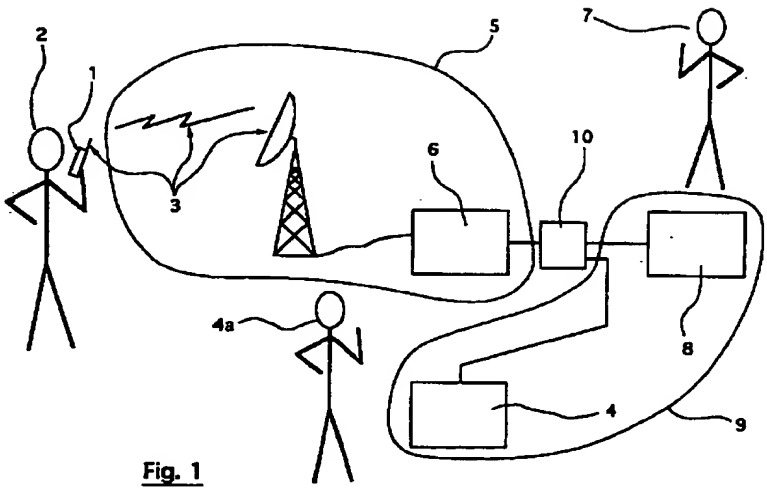

Fig. 1

【図２】

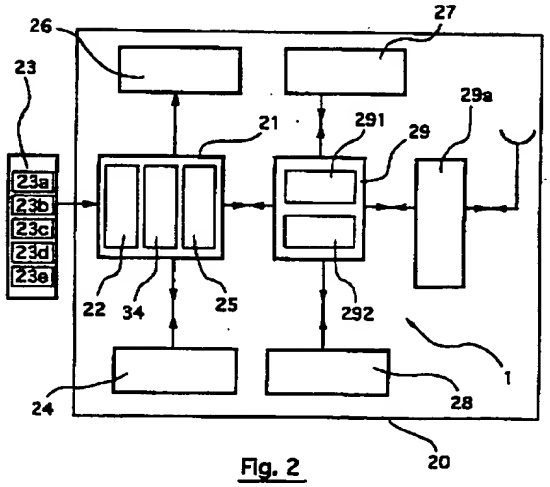

Fig. 2

【図３】

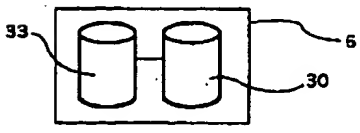

Fig. 3

【図４】

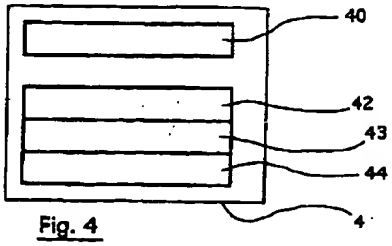

Fig. 4

【図５】

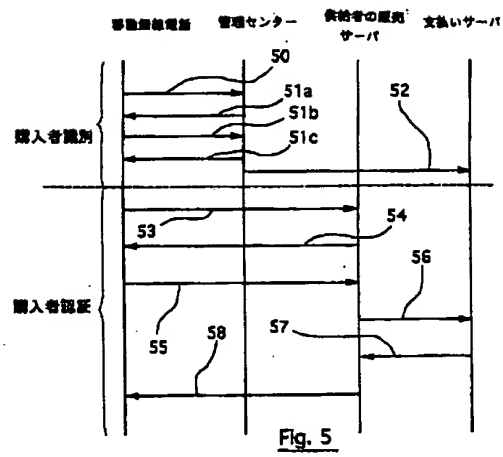

Fig. 5

【図６】

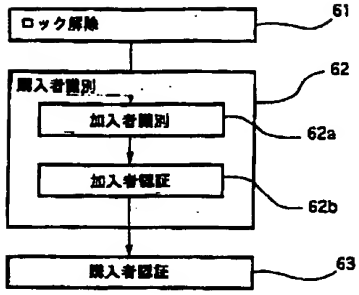

Fig. 6

【図７】

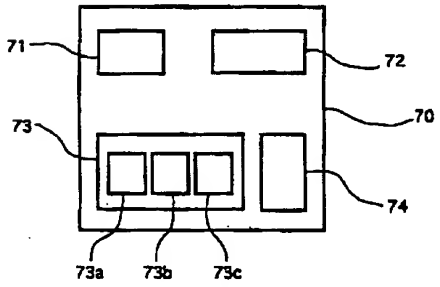

Fig. 7

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
		H04L 11/00	310B
		H04Q 7/04	H

(72)発明者 ソフィー・フレイ
フランス国、78100 サン・ジェルマン-アン・レイ、リュ・ドゥ・パリ 55
(72)発明者 アブダラ・イッティ
フランス国、78100 サン・ジェルマン-アン・レイ、リュ・デルメモン 34
(72)発明者 オリヴィエ・ジャン・マリー
フランス国、78490 バゾシュ、レザダン・マルタン 4
(72)発明者 フィリップ・リュカ
フランス国、91200 バレソー、リュ・ドゥ・ラッペ・ランベール 15
(72)発明者 フィリップ・メルシエ
フランス国、75013 パリ、リュ・ドゥ・レム 2
(72)発明者 ジャン・ピエール・ワリー
フランス国、92340 ブール・ラ・レーヌ、リュ・アンドレ・テュリエ 3

【外国語明細書】

1. Title of Invention

PROCESS FOR MAKING REMOTE PAYMENTS FOR THE PURCHASE OF GOODS AND/OR A SERVICE THROUGH A MOBILE RADIOTELEPHONE, AND THE CORRESPONDING SYSTEM AND MOBILE RADIOTELEPHONE

2. Claims

1. Process for remote and secure payment for goods and/or a service purchased by a buyer (2) from a supplier (7), making use of a mobile radiotelephone (1) used by the said buyer, the said mobile radiotelephone enabling access to a radio communications network (5) managed by a management center (6), a payment server (4) being connected to the said radio communications network (5),

characterized in that the said process includes the following step:

- identification (62) of the said buyer (2) by the said management center (6) and/or the said payment server (4) and/or a control center, the said buyer identification consisting of making sure that the buyer is a subscriber correctly registered on a list of subscribers to the said radio communications network (5).

2. Process according to claim 1, characterized in that the said buyer identification step (62) itself includes the following steps in sequence:

- subscriber identification (62a), enabling the said management center (6) and/or the said payment server (4) and/or the said control center to receive a subscriber identifier (IMSI; 23a; 50) specific to the said buyer, as a user of the said radio communications network;
- subscriber authentication (62b), enabling the said management center (6) and/or the said payment server (4) and/or the said control center to check the said subscriber identifier that was sent to it (them) during the said subscriber identification step (62a).

3. Process according to claim 2, characterized in that the said subscriber authentication step (62b) itself comprises the following steps:

- the said management center and/or the said payment server and/or the said control center supplies a random number (51a) to the said mobile radiotelephone;
- the said mobile radiotelephone generates a subscriber's electronic signature (51b):
  * with an individual authentication algorithm (23b) and/or an individual authentication key (23c) contained in protected areas (23) of the mobile radiotelephone (1), and
  * using the said random number;

- the mobile radiotelephone transmits the said subscriber's electronic signature to the said management center and/or to the said payment server and/or to the said control center;
- the said management center and/or the said payment server and/or the said control center checks the said subscriber's electronic signature.

4. Process according to any one of claims 1 to 3, characterized in that the said process also includes the following step:

- the said management center (6) and/or the said payment server (4) and/or the said control center authenticates (63) the said buyer (2), and possibly a decision to purchase the goods and/or service purchased by the buyer (2).

5. Process according to claim 4, characterized in that the said buyer authentication step, and possibly the purchase decision, itself comprises the following steps:

- the mobile radiotelephone generates a buyer's electronic signature;
- the mobile radiotelephone sends (29a) the said buyer's electronic signature to the said management center and/or the said payment server and/or the said control center;
- the said management center and/or the said payment server (4) and/or the said control center checks (42) the said buyer's electronic signature, the said buyer's electronic signature being kept (43, 44) available for use by the buyer and the supplier.

6. Process according to claim 4, characterized in that the said buyer authentication step, and possibly the purchase decision step, itself comprises the following steps:

- the buyer may input a confidential payment code into the mobile radiotelephone (1), using a keypad (24) associated with the mobile radiotelephone (1);
- the mobile radiotelephone sends a secure transmission of the said confidential payment code to the said management center and/or the said payment server and/or the said control center;
- the said management center and/or the said payment server (4) and/or the said control center checks the said confidential payment code.

7. Process according to claim 5, characterized in that the said buyer authentication step, and possibly the purchase decision, also comprises the following preliminary step:

- the buyer inputs a confidential payment code into the mobile radiotelephone (1) using a keypad (24) associated with the mobile radiotelephone (1).

8. Process according to either of claims 6 and 7 characterized in that the said step in which the said confidential payment code is input, is made using an input algorithm stored in the said mobile radiotelephone.

9. Process according to either of claims 6 and 7 characterized in that the said step in which the said confidential payment code is input, is made using at least one downloaded page in the HDML or an equivalent format provided for this purpose.

10. Process according to any one of claims 5 and 7 to 9, characterized in that the said step in which the buyer's electronic signature is generated is carried out:

- using a payment security algorithm (23d) and/or a payment security key (23e) contained in the protected areas (23) of the mobile radiotelephone (1), and
- starting from data about the transaction and/or data about the buyer.

11. Process according to claim 10, characterized in that at least some of the said data related to the transaction include a variability.

12. Process according to either of claims 10 and 11, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that the said payment security algorithm and/or the said payment security key is (are) stored in protected areas of the said terminal.

13. Process according to either of claims 10 and 11, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that the said payment security algorithm (23d) and/or the said payment security key (23e) is (are) stored in protected areas of the said subscriber identification module.

14. Process according to any one of claims 1 to 13, characterized in that it also comprises the following step:

- the mobile radiotelephone (1) is unlocked (61) if a comparison between a confidential identification code (PIN code) contained in protected areas (23) of the mobile radiotelephone (1), and a secret key known to the buyer and input by the buyer into the mobile radiotelephone using a keypad (24), is positive.

15. Process according to any one of claims 3, 10 and 12, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that at least one some of the said protected areas of the mobile radiotelephone (1) are included in the said subscriber identification module.

16. Process according to any one of claims 1 to 15, characterized in that it also comprises the following step:

- data related to payment for the purchase of goods and/or the service are encrypted (291), exchanged between the mobile radiotelephone and the management center and/or the payment server and/or the control center, to ensure that the purchase is confidential.

17. Process according to any one of claims 1 to 16, characterized in that it also comprises the following step:

- a check (292) of the integrity of data related to payment for the purchase of goods and/or the service exchanged between the mobile radiotelephone and the management center and/or the payment server and/or the control center, so that a defrauder is unable to modify the said data.

18. Process according to any one of claims 1 to 17, characterized in that the said buyer is associated with an electronic wallet (70) comprising:

- a wallet identifier (71) associated with a subscriber identifier (IMSI; 23a; 50) specific to the said buyer, as a user of the said radio communications network;
- means of payment (73, 73a, 73b, 73c);
- information (74) about the said buyer and/or the account(s) of the said buyer;

use of the said means of payment (73), particularly when buying goods and/or a service not being authorized until the buyer has been successfully identified (62), and possibly authenticated (63).

19. Process according to claim 18, characterized in that the said electronic wallet (70) also comprises:

- a confidential payment code (72) known to the said buyer.

20. Process according to either of claims 18 and 19, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that the said electronic wallet (70) is stored in one of the elements belonging to the group consisting of:

- the said terminal (20),
- the said subscriber identification module (23),
- the said payment server (4),
- the said management center (6),
- the said control center.

21. System for remote payment of goods and/or a service purchased by a buyer (2) from a supplier (7), in a secure manner using a mobile radiotelephone (1) used by the said buyer (2), the said mobile radiotelephone providing access to a radio communications network (5) managed by a management center (6), a payment server (4) being connected to the said radio communications network,
characterized in that the said system comprises means of implementing the process according to any one of claims 1 to 20.

22. Mobile radiotelephone (1) used by a buyer for remote payment of goods and/or a service purchased by a buyer (2) from a supplier (7), in a secure manner using a mobile radiotelephone (1) used by the said buyer (2), the said mobile radiotelephone providing access to a radio communications network (5) managed by a management center (6), a payment server (4) being connected to the said radio communications network,
characterized in that the said radiotelephone comprises means of implementing the process according to any one of claims 1 to 20.

3. Detailed Explanation of the Invention

This invention relates to a process for making remote payments for the purchase of goods and/or a service using a mobile radiotelephone. The invention also relates to a system and a mobile radiotelephone for embodiment of this process.

It is applicable to all types of mobile radiotelephones, in other words radiotelephones with a terminal only, and also mobile radiotelephones with a terminal that cooperates with a subscriber identification module.

In the GSM standard, the mobile radiotelephone (also called "mobile station") is of the second type, and the terminal and the subscriber identification module used in it are called the "mobile equipment" and "SIM (Subscriber Identity Module)" card respectively. Note that a SIM card is in the form of a microprocessor card that is slid into the mobile radiotelephone. It contains all individual information specific to the subscriber, and particularly the subscriber's International Module Subscriber Identity (IMSI), an individual authentication key (called Ki), and an individual authentication algorithm (called A3/A8).

Various electronic payment processes and systems have already been proposed.

Patent EP 451 057 B1, published on October 9 1991 describes a process and a system making use of a payment server. The solution recommended in this patent involves the use of a card that sends a voice identification signal. This signal is received by the telephone microphone and is then transmitted to the payment server.

Patent application WO 96/32701 published on October 17 1996 also describes an electronic payment process making use of a payment server. It can be used to make transactions related to the purchase of goods offered by merchants by means of IT services through an open computer telecommunications network, for example the "Internet" network, to which merchant server stations and customer stations and a payment server station, are connected.

For the purposes of this invention, it is assumed that remote payment for goods or services through a mobile radiotelephone is made through a closed type of radio communications network. A closed radio communications network refers particularly, but not exclusively, to networks based on the GSM technology (for example GSM 900, DCS 1800, etc.).

Note that a closed radio communications network may obviously by connected to one (or several) open network(s) through platforms or gateways. Thus, a user of the closed radio communications network can use his mobile radiotelephone to access an open network. For example, the "Internet" open network can be accessed using a mobile radiotelephone from a GSM network, if the mobile radiotelephone has the means (such as a navigator or browser) of using a protocol based on a specific language such as the HDML (Handset Device Markup Language) or WML (Wireless Markup Language) or any other language of the same type and/or derived from one of the two above mentioned languages.

Due to the fact that a closed radio communications network does not enter into the category of open computer telecommunications networks, the solution recommended by application WO 96/32701 cannot be applied to the problem that arises with the invention (specifically remote payment for goods or services using a mobile radiotelephone).

The purpose of this invention is precisely to provide a process for secure remote payment for goods and/or a service purchased from a supplier, making use of a mobile radiotelephone.

Another purpose of this invention is to supply this type of payment process to minimize work done by the buyer, while offering optimum security.

These various objectives, and others that will appear later, are achieved according to the invention by means of a process for remote and secure payment for goods and/or a service purchased by a buyer from a supplier, making use of a mobile radiotelephone used by the said buyer, the said mobile radiotelephone enabling access to a radio communications network managed by a management

center, a payment server being connected to the said radio communications network, the said process comprising the following step:

- identification of the said buyer by the said management center and/or the said payment server and/or a control center, the said buyer identification consisting of making sure that the buyer is a subscriber correctly registered on a list of the subscribers to the said radio communications network.

Thus, at the end of this buyer identification step, the payment server manager is assured that the buyer is a bona fide member of the radio communications network to which the payment server is connected.

Note that if the buyer is identified by the radio communications network management center, the radio communications operator (who is responsible for operation of this management center) becomes a "semi-trusted third party" towards the bank organization (which is responsible for operation of the payment server), within the framework of this invention. In this case the bank organization simply authenticates the buyer, the operator being responsible for the identification of the person in possession of the mobile radiotelephone.

Preferably, the said buyer identification step itself includes the following steps in sequence:

- subscriber identification, enabling the said management center and/or the said payment server and/or the said control center to receive a subscriber identifier specific to the said buyer, as a user of the said radio communications network;
- subscriber authentication, enabling the said management center and/or the said payment server and/or the said control center to check the said subscriber identifier that was sent to it (them) during the said subscriber identification step.

Thus, during the first buyer identification step, advantage is taken of the fact that the subscriber in a closed radio communications network (for example of the GSM type) must be identified and authenticated by the operator responsible for the charging system, to prevent fraud and to ensure that billing is correct. Therefore, the security provided by the physical layers of a closed network, for example of a GSM type, is astutely used. Note that in an open network, for example such as Internet, security is applied at application level.

Preferably, the said subscriber authentication step itself comprises the following steps:

- the said management center and/or the said payment server and/or the said control center supplies a random number to the said mobile radiotelephone;
- the said mobile radiotelephone generates a subscriber's electronic signature:
  * with an individual authentication algorithm and/or an individual authentication key contained in protected areas of the mobile radiotelephone, and
  * using the said random number;
- the mobile radiotelephone transmits the said subscriber's electronic signature to the said management center and/or to the said payment server and/or to the said control center;
- the said management center and/or the said payment server and/or the said control center checks the said subscriber's electronic signature.

Thus the subscriber authentication procedure specified in the GSM standard is used during the buyer identification step. It is important to note that the subscriber authentication procedure must in no case be confused with the buyer authentication procedure.

Preferably, the said process also comprises a step in which the said management center and/or the said payment server and/or the said control center authenticates the said buyer, and possibly a decision to buy the goods and/or service purchased by the buyer.

Thus, at the end of this buyer authentication step, the payment server manager is assured that the buyer is authorized to pay for the purchased goods and/or services. Therefore, the payment server manager can authorize the payment, or make compensation movements between the buyer's account and the supplier's account.

In one preferred embodiment of the invention, the said buyer authentication step, and possibly the purchase decision, itself comprises the following steps:

- the mobile radiotelephone generates a buyer's electronic signature;
- the mobile radiotelephone transmits the said buyer's electronic signature to the said management center and/or the said payment server and/or the said control center;
- the said management center and/or the said payment server and/or the said control center checks the said buyer's electronic signature, the said

buyer's electronic signature being kept available for use by the buyer and the supplier.

According to one advantageous variant, the said buyer authentication step, and possibly the purchase decision step, itself comprises the following steps:

- the buyer may input a confidential payment code into the mobile radiotelephone, using a keypad associated with the mobile radiotelephone;
- the mobile radiotelephone sends a secure transmission of the said confidential payment code to the said management center and/or the said payment server and/or the said control center;
- the said management center and/or the said payment server and/or the said control center checks the said confidential payment code.

Thus, according to this variant, there is no need to calculate a signature. For example, a secure transmission could be a transmission in an encrypted form.

Advantageously, the said buyer authentication step, and possibly the purchase decision, also comprises a step in which the buyer inputs a confidential payment code into the mobile radiotelephone by means of a keypad associated with the mobile radiotelephone; in particular, the said buyer's electronic signature may be generated as a function of the said confidential payment code.

This optional step increases the security with which the buyer is authenticated.

Two advantageous embodiments of this step for inputting the confidential payment code may be considered.

In a first variant, this step is carried out using an input algorithm stored in the said mobile radiotelephone. Thus in this first variant, the radiotelephone permanently stores the input algorithm (in the terminal and/or the subscriber identification module). Therefore, it requires a few modifications within the radiotelephone (in the terminal and/or the subscriber identification module).

In the second variant, this step is carried out using at least one downloaded page in the HDML or an equivalent format provided for this purpose. Thus, in this second variant, the radiotelephone contains no permanent storage for any input algorithm.

Preferably, the said step in which a buyer's electronic signature is generated is made with a payment security algorithm and/or a payment security key contained in protected areas of the mobile radiotelephone, starting from data related to the transaction and/or data about the buyer.

Note that the buyer's electronic signature authenticates either the buyer alone or the buyer and the buying decision, depending on whether or not it takes account of data related to the transaction. It can be used to arbitrate about disputes between the buyer and/or the supplier and/or the payment server. It is essential if a dispute arises.

Advantageously, at least some of the said data related to the transaction include variability.

Advantageously, the said payment security algorithm and/or the said payment security key is (are) stored in protected areas of the said terminal. According to one advantageous variant, data is stored in protected areas of the said subscriber identification module.

Advantageously, the said process also comprises the following step: the mobile radiotelephone is unlocked if a comparison between a confidential identification code contained in protected areas of the mobile radiotelephone, and a secret key known to the buyer and input by the buyer into the mobile radiotelephone using a keypad, is positive.

This "unlocking" (also called "initialization") of the mobile radiotelephone is an additional optional verification known in itself, and offered by some operators, particularly in GSM type networks. Note that the Personal Identity Number (or PIN code) is input by the subscriber, for example each time that the subscriber identification module is inserted into the terminal, or each time that the terminal is switched on.

Preferably, at least some of the said protected areas of the mobile radiotelephone are contained in a subscriber identification module.

For security reasons, in order to make the terminal as independent as possible from the user, it is preferable to confine a maximum amount of personal and confidential information (algorithm and individual authentication key, payment algorithm and security key, etc.) in the subscriber identification module.

Advantageously, the said process also comprises a step in which data related to payment for the purchase of goods and/or the service are encrypted, exchanged between the mobile radiotelephone and the management center and/or the payment server and/or the control center, to ensure that the purchase is confidential.

Advantageously, the said process also comprises a step to check the integrity of data related to payment for the purchase of goods and/or the service exchanged between the mobile radiotelephone and the management center and/or

the payment server and/or the control center, so that a defrauder is unable to modify the said data.

In a preferred embodiment of the invention, the said buyer is associated with an electronic wallet comprising:

- a wallet identifier associated with a subscriber identifier specific to the said buyer, as a user of the said radio communications network;
- means of payment;
- information about the said buyer and/or the account(s) of the said buyer;

use of the said means of payment, particularly when purchasing goods and/or a service not being authorized until the buyer has been successfully identified, and possibly authenticated.

Identification and authentication (if necessary) of the buyer may also be seen as identification and authentication (if applicable) of this buyer's electronic wallet. Several cases may arise, such as for example:

- a subscriber (and a corresponding subscriber identification module) is associated with a single electronic wallet;
- several subscribers (and therefore several corresponding subscriber identification modules) share the same electronic wallet (for example the case of a company holding the wallet);
- the same subscriber (and the corresponding subscriber identification module) is associated with several electronic wallets.

Note that, due to the correlation between the wallet identifier and the subscriber identifier (the subscriber being the buyer), the identification of the buyer (as a subscriber) provides an implicit identification of his electronic wallet. Note that in the third case mentioned above, one of the subscriber's electronic wallets may for example be chosen by default or, as a variant, the buyer may be offered the possibility of making a choice from the several electronic wallets available to him.

After identification, and possibly after authentication, the buyer may use the payment means contained within his electronic wallet.

Advantageously, the said electronic wallet also comprises a confidential payment code known to the said buyer. Note that this confidential payment code input by the buyer using the radiotelephone keypad, may be used during the calculation of the buyer's electronic signature, so that the buyer and possibly the buying decision, can be authenticated.

Preferably, the said electronic wallet is stored in one of the elements belonging to the group consisting of the said terminal, the said subscriber identification module, the said payment server, the said management center and the said control center.

In other words, various locations of the electronic wallet may be considered without going outside the framework of this invention.

The invention also relates to a system for secure remote payment of goods and/or a service purchased by the buyer from a supplier, using a mobile radiotelephone used by a buyer.

The invention also relates to a mobile radiotelephone used by a buyer for secure remote payment of goods and/or a service purchased by the buyer from a supplier.

This system and this radiotelephone according to the invention comprise means of embodying the process mentioned above.

Other characteristics and advantages of the invention will become obvious from reading the following description of different variant embodiments of the invention, given for information and for non-restrictive purposes, and the attached drawings in which:

- figure 1 shows a diagrammatic overall view of a particular embodiment of a system according to the invention;
- figure 2 shows a view of a particular embodiment of a mobile radiotelephone according to the invention, in the form of a block diagram;
- figure 3 shows a view of a particular embodiment of a management center according to the invention, in the form of a block diagram;
- figure 4 shows a view of a particular embodiment of a payment server according to the invention, in the form of a block diagram;
- figure 5 contains an organization chart showing the steps of operations related to the purchase of goods and/or a service;
- figure 6 contains a simplified flowchart showing a particular embodiment of the process according to the invention; and
- figure 7 shows a view of a particular embodiment of an electronic wallet according to the invention, in the form of a block diagram.

Therefore the invention relates to a process, and a corresponding system and mobile radiotelephone, that a buyer can use to make remote payments for the purchase of goods and/or a service, using a mobile radiotelephone.

In the particular embodiment shown in figure 1, the system comprises a mobile radiotelephone 1 enabling access to a radio communications network 5 (for example a GSM network) managed by a management center 6, through a radio relay link 3. A payment server 4 and a sales server 8 are also connected to the radio communications network 5.

In the example presented, the payment server 4 and the sales server 8 are connected to an open computer telecommunications network, for example the Internet network 9. The radio communications network 5 is interconnected to this Internet network 9, through a gateway 10 (for example a UP access platform marketed by the Unwired Planet Company). In this case the mobile radiotelephone is provided with a navigator (for example a "UP browser" (registered trademark) navigator marketed by the Unwired Planet Company) which enables it to navigate through the gateway within the Internet network and particularly to access the payment server 4 and the sales server 8.

The system enables a buyer 2 provided with a mobile radiotelephone 1, and therefore in this case also assumed to be a subscriber registered with the radio communications network operator 5, to make a secure remote payment for goods and/or a service that he has purchased from a supplier 7 who has a remote sales server 8.

In the particular embodiment presented in figure 2, the mobile radiotelephone 1 comprises a terminal 20 that works in cooperation with a SIM card 23. However, it is obvious that this invention is also applicable to a radiotelephone consisting of the terminal alone (in other words not including the subscriber identification module).

In a manner known in itself, the terminal 20 may for example include a communication management module 21 and an information processing module 29, around which a keypad 24, a display screen 26, a loudspeaker 27, a microphone 28 and radio transmission-reception means 29a (including an antenna) are interconnected.

It is obvious that the information is also more generally applicable to any type of mobile radiotelephone. Thus, the "conventional" terminal as described above may be replaced by any type of radio communications module that can be connected to a radio communications network, for example like a terminal without a keypad or a screen, or a microcomputer working together with a terminal through a PCMCIA ("Personal Computer Memory Card International Association") or equivalent type of card.

The process according to the invention comprises the following steps, as shown in the flowchart in figure 6:

- (optionally) unlock (61) (or initialize) the mobile radiotelephone 1;
- the management center 6 and/or the payment server 4 and/or an independent control center (not shown) identifies (62) the buyer as a user of the radio communications network;
- (optionally) the management center 6 and/or the payment server 4 and/or the control center (not shown) authenticates (63) the buyer, and possibly a purchase decision made by the buyer to purchase goods and/or a service.

The (optional) step 61 in which the radiotelephone 1 is unlocked is known in itself, and may for example take place as follows: the buyer 2 inputs a personal identity number (or PIN code according to GSM terminology) on the keypad 4, then the radiotelephone 1 compares the personal identity number input by the buyer with the personal identity number stored in protected areas in the mobile radiotelephone 1 (typically in the SIM card 23). The radiotelephone 1 is not "unlocked" (in other words made operational in the radio communications network) unless the comparison is positive.

The step 62 in which the buyer 2 is identified according to this invention, consists of identifying and authenticating the subscriber, who is the buyer when he uses the radiotelephone. Therefore, for example this step 62 includes the following conventional steps:

- subscriber identification (62a), by which the management center 6 receives a subscriber identifier specific to the buyer as a user of the radio communications network. The subscriber identifier 23a, or IMSI according to the GSM terminology, is typically stored in the SIM card 23;
- subscriber authentication (62b), allowing the management center to check the subscriber identifier sent to it in subscriber identification step 62a.

Note that the buyer identification step (consisting of a subscriber identification and authentication) is carried out automatically, in other words it requires no action by the buyer. The buyer only takes part in the next step of buyer authentication, when he is asked to input his confidential payment code.

It is also important to note that the subscriber authentication step 62b must in no case be confused with the buyer authentication step 63 presented in detail

below. Authentication of the subscriber (who is the buyer) only takes place for the purpose of buyer identification. It can be understood that this buyer identification then needs to be used together with buyer authentication, so that the payment server verifies that the identified buyer is authorized to make purchases.

As an example only, refer to figure 5 which shows the "conventional" procedure used in GSM for these subscriber identification 62a and authentication 62b steps. The radiotelephone 1 sends the user's subscriber identifier (IMSI) 50 to the management center 6. After the subscriber has thus been identified (62a), the management center 6 must check his identity, in other words must authenticate him (62b). This is done by the management center 6 supplying a random number ("RAND") 51a to the radiotelephone 1. Starting from this random number, and using an algorithm ("A3/A8") 23b and an individual authentication key ("Ki") 23c contained in protected areas of the mobile radiotelephone (typically the SIM card 23), the radiotelephone 1 calculates a subscriber's electronic signature ("SRES"). This subscriber's electronic signature 51b is sent to the management center 6 (and more precisely to a subscriber management module 30) which checks it by comparing it with the signature that it calculated locally. If the two subscriber's electronic signatures are identical, the subscriber authentication (and for the purposes of the invention, the buyer identification) is successful (the person holding the mobile radiotelephone 1 is on the subscribers list) and the management center sends messages 51c and 52 to confirm this to the radiotelephone 1 and to an identification module 40 located in the payment server. Furthermore, the GSM technology enables independent authentication of the communication set up as a function of the network topology (when setting up, during a handover, etc.).

In summary, after execution of the buyer identification step 62, the manager 4a of the payment server 4 is assured that the person 2 holding the mobile radiotelephone 1 (in other words the buyer in this case) is correctly registered on the subscribers list, and therefore that he is a bona fide member of the radio communications network to which the payment server 4 is connected.

The buyer identification step 62 may be followed by a buyer authentication step 63. In this step, the manager 4a of the payment server 4 assures itself that the buyer 2 in possession of the mobile radiotelephone 1 at the time of the payment is authorized to pay for the purchased goods and/or services. If so, the payment server manager can then authorize payment or make compensation movements between the buyer's account 2 and the supplier's account 7. This buyer

authentication step 63 may be used before or after the buyer has made the purchase decision.

In one particular embodiment, the buyer authentication step 63 comprises the following steps:

- (optionally) the buyer 2 uses the keypad 24 on the mobile radiotelephone 1 to input a confidential payment code. For example, this input step may be carried out using an input algorithm stored in the mobile radiotelephone (in the SIM card 23 or in the terminal 20), or according to one variant, using one or several downloaded pages in the HDML or equivalent format, and provided for this purpose;
- the mobile radiotelephone generates a buyer's electronic signature:
  - with an algorithm 23d and a payment security key 23e contained in the protected areas 23 of the mobile radiotelephone (either in the terminal 20 or in the SIM card 23);
  - starting from data about the transaction (such as the contents and/or the price) and/or data about the buyer (such as the confidential payment code, if the buyer had input the payment code). Furthermore, data about the transaction may include elements supplying variability on the signature (for example such as the time date of the transaction, a random number, a transaction serial number, etc.);
- the mobile radiotelephone 1 transmits the buyer's electronic signature to the payment server 4;
- the buyer's electronic signature is checked in a check module 42 included in the payment server 4. The buyer's electronic signature is kept available to the buyer 2 and the supplier 7. This check may also be carried out by the subscriber management center 6 or by the control center (not shown). In the former case, the subscriber management center 6 comprises an authentication module 33 for radiotelephone holders subscribing to the remote payment service.

The procedure adopted in this particular embodiment (given as an example) of the buyer authentication step then continues (refer to the lower part of figure 5). The buyer 2 sends a purchase request 53 to the sales server 8 of the supplier 7. In return, he receives data about the price of the goods and/or service 54. The buyer then makes a purchase decision 55. At the same time, the calculation means (typically a microprocessor) in the mobile radiotelephone calculate a buyer's electronic signature. The mobile radiotelephone 1 uses transmission means 29a to

send the buyer's purchase decision and his electronic signature firstly to the server 8 of the supplier 7 (arrow marked 55) and secondly to the payment server 4 (arrow marked 56). The payment server 4 includes a check module (or certification module) 42 to check (or certify) the buyer's electronic signature. This check module 42 checks the signature, for example by carrying out calculations with operations exactly the same as those carried out in the mobile radiotelephone at the time of the purchase. If the payment server 4 accepts the transaction, a "transaction accepted" message 57 is sent to the supplier's server 8 through a reception acknowledgment module 43 on the payment server 4. The supplier's server 8 sends a "purchase confirmation" message 58 to the buyer (to the buyer's mobile radiotelephone and/or the buyer's home). The buyer's electronic signatures are stored by a storage module 44 on the payment server 4 and are kept available to the buyer and the supplier.

It is obvious that if the subscriber management center 6 or the control center (not shown) checks (or certifies) the buyer's electronic signature, then the subscriber management center or the control center will include checking, acknowledgment and storage type modules like 42, 43 and 44 described above for the payment server 4.

According to another variant that is easier to implement, the buyer authentication step 63, and possibly the purchase decision itself, includes the following steps:

- the buyer inputs a confidential payment code into the mobile radiotelephone 1 using the keypad 24 associated with the mobile radiotelephone. This input step may for example be carried out using an input algorithm stored in the mobile radiotelephone (in the SIM card 23 or in the terminal 20) or according to one variant, using one or several downloaded pages in the HDML format or equivalent format provided for this purpose;
- the mobile radiotelephone makes a secure transmission of the confidential payment code to the payment server 4;
- the payment server 4 checks the confidential payment code (for example by verifying that this confidential payment code actually belongs to a predetermined list of valid payment codes).

Regardless of what embodiment is chosen, after the buyer authentication step 63, the manager 4a of the payment server 4 is assured that the buyer 2 in possession of the mobile radiotelephone 1 at the time of the payment is authorized

to pay for the purchased goods and/or services. The buyer's electronic signature is sufficient to arbitrate any disputes that may arise between the buyer 2 and/or the supplier 7 and/or the manager 4a of the payment server 4.

According to this invention, the radiotelephone 1, for example in the communications management module 21, comprises various means necessary for implementing the various steps in the process as described above (through several implementations and variants). In particular, the radiotelephone comprises means 22 necessary for unlocking the radiotelephone, means 34 necessary for identifying the buyer, and means 25 necessary for authenticating the buyer.

The communication management means and/or information processing means 29 of the mobile radiotelephone 1 may also comprise means 291 of encrypting data about payment for the purchase of goods and/or services exchanged between the mobile radiotelephone 1 and/or the management center 6 and/or the payment server 4 and/or the control center, in a manner known in itself. These encryption means assure confidentiality of the purchase.

Information processing means 29 of the mobile radiotelephone 1 may also comprise means 292 of controlling the integrity of data related to payment for the purchase of goods and/or services, exchanged between the mobile radiotelephone 1 and/or the management center 6 and/or the payment server 4 and/or the control center, in a manner known in itself. Thus, a defrauder is unable to modify these data.

Furthermore, according to this invention, each buyer may be associated with an electronic wallet 70. A shown in figure 7, this wallet 70 may for example comprise:

- a wallet identifier 71 associated with a subscriber identifier (for example the subscriber's "IMSI") specific to the buyer (as a user of the radio communications network);
- a confidential payment code 72, known only to the buyer 2;
- payment means 73, particularly but not exclusively an electronic wallet 73a (usually for amounts less than a predetermined threshold), a credit card holder 73b (usually for amounts greater than the above mentioned predetermined threshold), or any other payment means 73c available to the buyer provided by bank organizations.
- information 74 about the buyer and/or his account(s).

Use of payment means 73 is only authorized, particularly when purchasing goods and/or a service, after successful identification and possibly authentication of the buyer 2.

This electronic wallet may be stored in various locations, namely in the terminal 20, in the SIM card 23, in the payment server 4, in the management center 6 or in the control center (not shown).

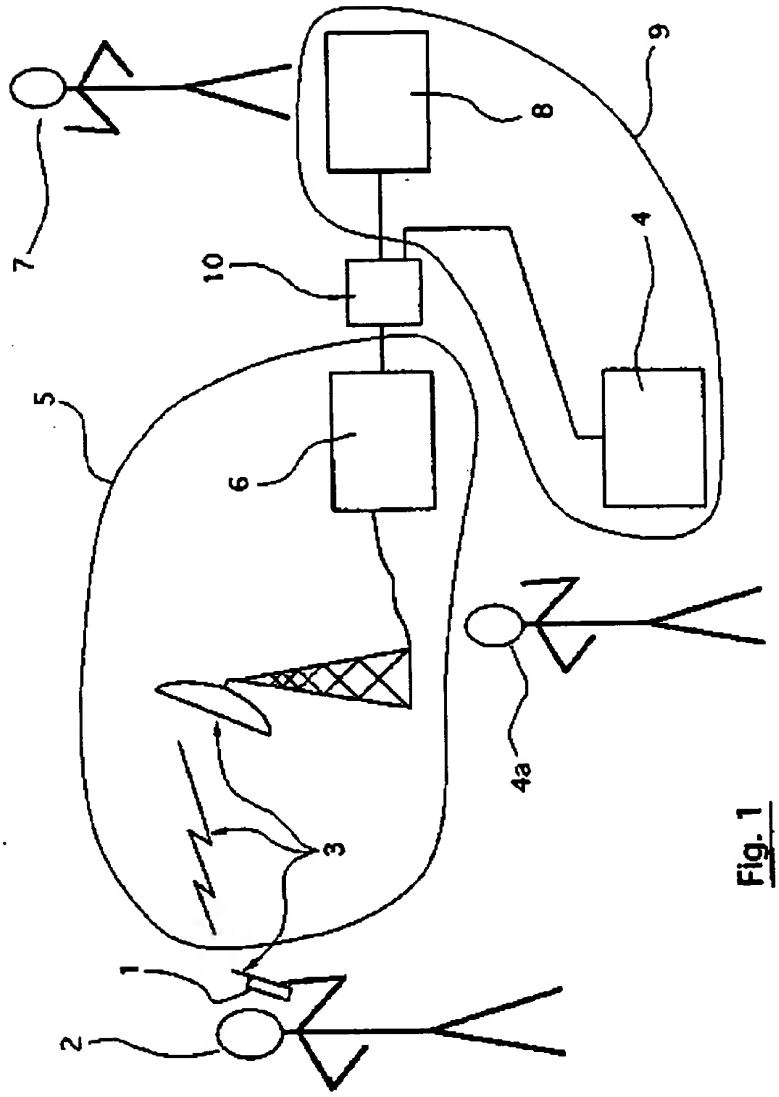

Fig. 1

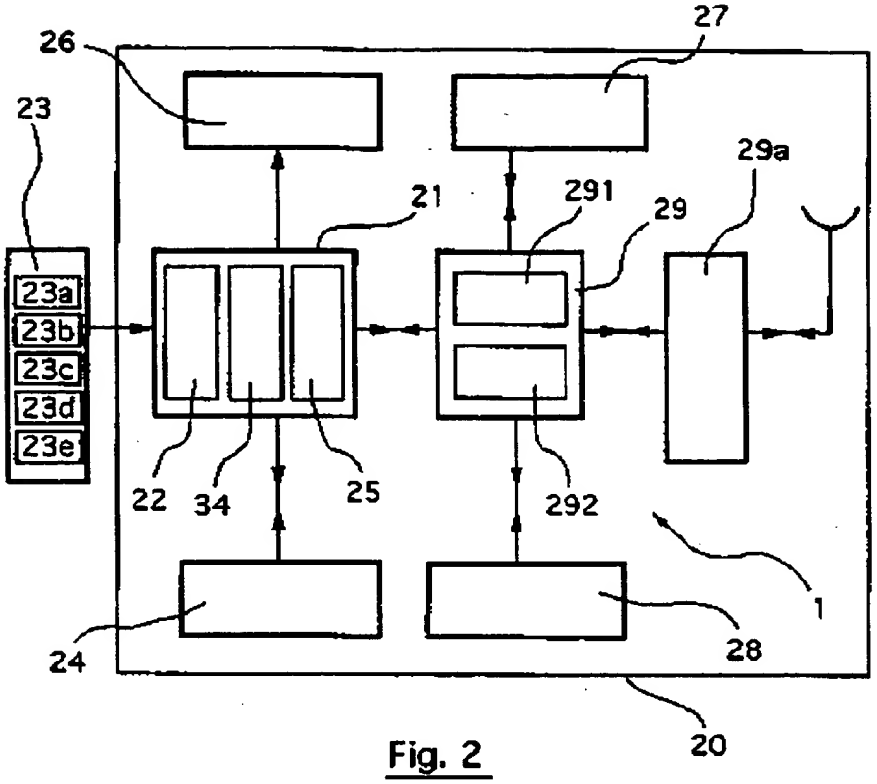
26
27
23
29a
21
291
29
23a
23b
23c
23d
23e
22
34
25
292
1
24
28
20

Fig. 2

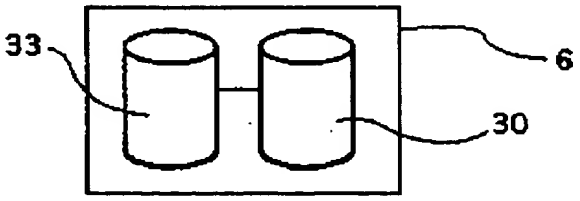
33
6
30

Fig. 3

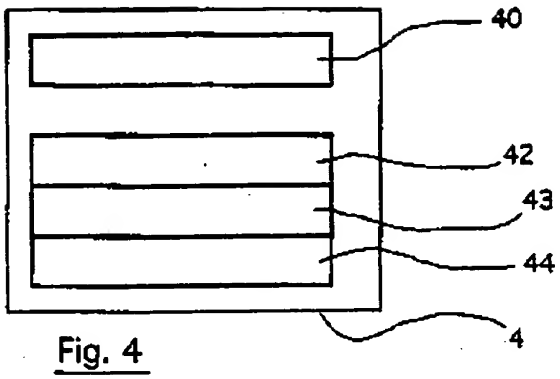
40
42
43
44
4

Fig. 4

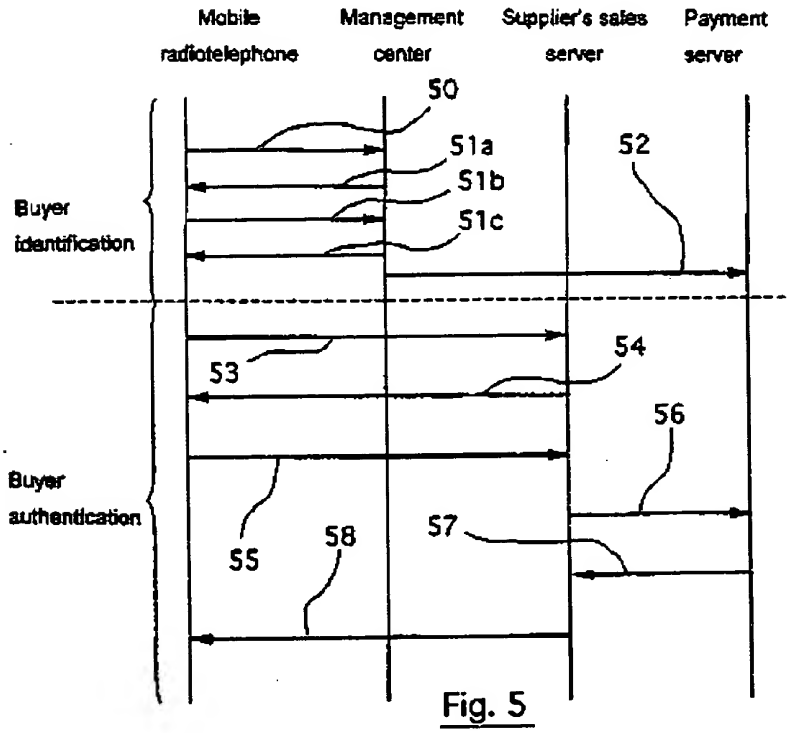
Mobile radiotelephone
Management center
Supplier's sales server
Payment server
50
51a
51b
51c
52
Buyer identification
53
54
56
Buyer authentication
55
58
57

Fig. 5

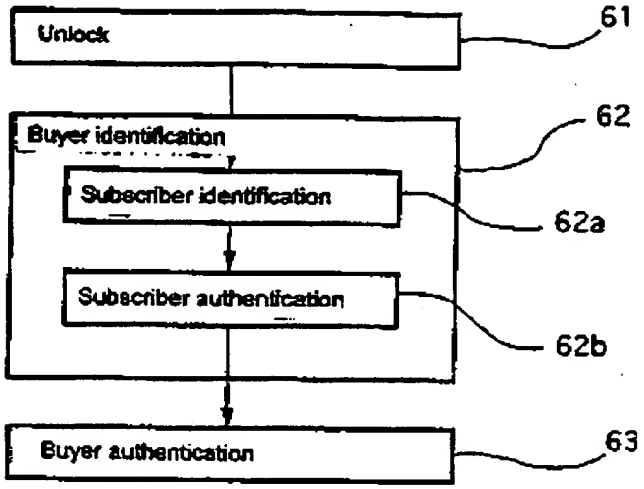
Unlock
61
Buyer identification
62
Subscriber identification
62a
Subscriber authentication
62b
Buyer authentication
63

Fig. 6

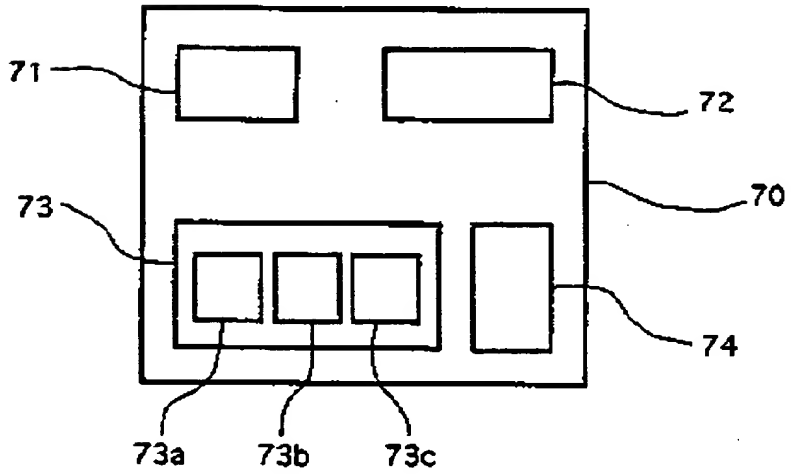
71
72
70
73
74
73a
73b
73c

Fig. 7

1. Abstract

The invention relates to a process for making a secure remote payment for goods and/or a service purchased by the buyer (2) from a supplier (7) using a mobile radiotelephone (1) used by the buyer. The mobile radiotelephone provides access to a radio communications network (5) managed through a management center (6). A payment server (4) is connected to the radio communications network (5). The process according to this invention comprises a step in which the said management center (6) and/or the said payment server (4) and/or a control center identifies the said buyer (2), identification of the buyer consisting of ensuring that the buyer is a bona fide subscriber registered on a list of subscribers to the said radio communications network (5). The process may also include a step to authenticate the said buyer (2).

Figure 1.

This Page Blank